

NOT FOR PUBLICATION

FILED

UNITED STATES COURT OF APPEALS

AUG 21 2024

FOR THE NINTH CIRCUIT

MOLLY C. DWYER, CLERK
U.S. COURT OF APPEALS

MICHAEL GREENSTEIN; CYNTHIA
NELSON; SINKWAN AU, individually and
on behalf of themselves and all other persons
similarly situated,

Plaintiffs-Appellants,

v.

Noblr Reciprocal Exchange, a Colorado
corporation,

Defendant-Appellee.

No. 22-17023

D.C. No.
4:21-cv-04537-JSW

MEMORANDUM*

Appeal from the United States District Court
for the Northern District of California
Jeffrey S. White, Senior District Judge, Presiding

Argued and Submitted February 14, 2024
San Francisco, California

Before: MILLER, BADE, and VANDYKE, Circuit Judges.

Plaintiffs-Appellants Michael Greenstein, Cynthia Nelson, and Sinkwan Au
filed this putative class action against Defendant-Appellee Noblr Reciprocal
Exchange after their driver's license numbers were targeted in a cyberattack. The

* This disposition is not appropriate for publication and is not precedent except as
provided by Ninth Circuit Rule 36-3.

attackers, whose identities remain anonymous, conducted the attack by manipulating Noblr's online insurance quote system to gain access to an unknown number of victims' driver's license numbers. Greenstein and Nelson have not alleged any misuse of their driver's license numbers after the attack, while Au has alleged that her driver's license number was used in an unsuccessful application for New York unemployment benefits shortly thereafter. Plaintiffs allege negligence and violations of federal and state consumer protection law, 18 U.S.C. § 2724 ("DPPA"), Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL"). They seek damages as well as declaratory and injunctive relief.

After Noblr filed its first motion to dismiss, the district court dismissed Plaintiffs' claims on standing grounds with leave to amend. Plaintiffs amended their class complaint in response, and Noblr again moved to dismiss. The district court again dismissed Plaintiffs' claims for lack of standing, this time with prejudice. "We review a district court's dismissal under Rule 12(b)(1) for lack of standing *de novo*," *Unified Data Servs., LLC v. Fed. Trade Comm'n*, 39 F.4th 1200, 1209 (9th Cir. 2022), and we affirm.

To establish standing, a plaintiff must allege an injury in fact that is fairly traceable to the defendant and likely redressable by a favorable judicial decision. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). The injury must be "concrete, particularized, and actual or imminent." *TransUnion LLC v. Ramirez*, 594 US. 413,

423 (2021). “On appeal from a motion to dismiss, a plaintiff need only show that the facts alleged, if proven, would confer standing.” *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1141 (9th Cir. 2010).

Plaintiffs argue they have satisfied their burden to plead an injury in fact by alleging an increased risk of future identity theft stemming from the cyberattack. Under *Krottner*, plaintiffs “whose personal information has been stolen but not misused” can establish injury if they “face[] a credible threat of harm, and that harm is both real and immediate, not conjectural or hypothetical.” *Id.* at 1143 (internal quotation marks and citations omitted). Put another way, “the sensitivity of the personal information, combined with its theft,” can establish an injury when it creates “a substantial risk that the [] hackers will commit identity fraud or identity theft” in the future. *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027, 1029 (9th Cir. 2018).

Here, however, Plaintiffs cannot rely on the future risk of identity theft to establish an actual or imminent injury because unlike the plaintiffs in *Krottner* and *Zappos*, they have not adequately alleged their driver’s license numbers were among those stolen in the attack on Noblr’s quote system. Their allegations rely heavily on a notice Noblr sent to 97,633 individuals—including Plaintiffs—several months after the attack. But the description of the attack provided in the Notice, which accounts for the bulk of the factual allegations included in the complaint, is

ultimately insufficient to establish that Plaintiffs' driver's license numbers were stolen.

While the Notice does confirm that "the attackers were able to access driver's license numbers," it stops short of confirming that any individual recipient of the Notice had his or her driver's license number stolen. It does not confirm which or how many driver's license numbers were accessed, nor does it confirm whether the driver's license numbers of all 97,633 recipients of the Notice were taken from Noblr's website. Instead, in explaining "[w]hat [i]nformation [w]as [i]nvolved," the Notice states only that each recipient's "name, driver's license number, and address *may* have been accessed." (emphasis added). After reading the Notice, all that a reasonable reader would know for certain is that Noblr suffered a cyberattack, some driver's license numbers were taken as a result, and his own driver's license number may (or may not) have been among those stolen. Aside from the factual allegations pulled from the Notice, Plaintiffs provide no additional allegations that might provide a credible basis to conclude their driver's license numbers were taken.¹

¹ Plaintiffs' contention that their driver's license numbers were published in Noblr's website's source code and publicly available to steal en masse, for example, is contradicted by the version of events included in the Notice, which explains that the attack was conducted by manipulating the online quote system on an individual, query-by-query basis that would have required the hackers to already have other personal information about the victims in their possession. *See Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001) (explaining that the court need not accept as true allegations that are contradicted).

Plaintiffs’ allegations reflect the uncertainty associated with the version of events contained in the Notice. For example, Plaintiffs assert that “at least 97,633 people were affected” by the cyberattack, but they do not explain in what manner each person was “affected.” Likewise, throughout the complaint Plaintiffs allege that Noblr “exposed” their driver’s license numbers to third parties, but an “exposed” driver’s license number is different from a “stolen” one. In similar fashion, Plaintiffs state that their “driver’s license number[s] and address[es] *may* have been accessed,” and frame the “actual injury” they suffered as stemming “from having [their] PI *exposed*”—not from having it stolen. (emphasis added).

It is true that elsewhere in the complaint, Plaintiffs include at least some affirmative allegations that their driver’s license numbers were stolen. But these allegations are conclusory and unsupported by their heavy reliance on the facts contained in the Notice. Au, for example, alleges explicitly that “her driver’s license number was stolen shortly before she experienced [the] fraudulent unemployment claim.” And all three Plaintiffs allege that “the thieves ... exfiltrate[d] individuals’ PI” and that “Plaintiffs[’] ... PI was taken.” These definitive conclusions are unwarranted in light of the uncertain version of events on which Plaintiffs have built their complaint. “[T]he court [is not] required to accept as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences.” *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1008 (9th Cir. 2018).

Where, as here, Plaintiffs have not sufficiently alleged that their personal information was actually stolen, they cannot rely on the increased risk such a theft might have posed had it occurred. In *Krottner*, our court noted that we would “find the threat far less credible” if the plaintiffs’ “allegations [were] more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs had sued based on the risk that it would be stolen at some point in the future.” 628 F.3d at 1143. This case presents the kind of “far less credible” allegations envisioned by *Krottner*. Plaintiffs’ standing argument, which is ultimately premised on a “speculative chain of possibilities” about the potential consequences stemming from the manipulation of Noblr’s online quote system, does not satisfy their burden of pleading an actual or imminent injury. *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 414 (2013).

Because Plaintiffs have not established a sufficient risk of future harm, their argument that they have alleged separate concrete harms stemming from that risk also fails. Only when the risk of future harm is not speculative can the cost of mitigation efforts form a basis for standing. Having alleged only a speculative risk of harm, Plaintiffs “cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.” *Clapper*, 568 U.S. at 416.

Nor does the DPPA provide a basis for standing. Although Congress can “elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law,” *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 578 (1992), plaintiffs seeking to establish standing for such statutory harms must “identif[y] a close historical or common-law analogue for their asserted injury,” *TransUnion LLC*, 594 U.S. at 424. Plaintiffs seek to analogize their claims under the DPPA to the common law torts of intrusion upon seclusion, invasion of privacy, and public disclosure of private facts. But the disclosure of driver’s license numbers is neither “highly offensive,” *Hernandez v. Hillsides, Inc.*, 211 P.3d 1063, 1072 (Cal. 2009) (intrusion upon seclusion), “an egregious breach of the social norms,” *id.* at 1073 (quoting *Hill v. Nat’l Collegiate Athletic Ass’n*, 865 P.2d 633, 655 (Cal. 1994)) (invasion of privacy), nor “offensive and objectionable to the reasonable person,” *Shulman v. Grp. W Prods., Inc.*, 955 P.2d 469, 478 (Cal. 1998) (quoting *Diaz v. Oakland Trib., Inc.*, 188 Cal. Rptr. 762, 768 (Ct. App. 1983)) (public disclosure of private facts).

Even assuming Plaintiff Au sufficiently pled injury by alleging that her driver’s license number was used in the fraudulent application for unemployment benefits in New York, Au has failed to establish that such injury is “‘fairly traceable’ to the conduct being challenged.” *Zappos*, 888 F.3d at 1029.

First, the unknown third parties who conducted the attack would have needed to possess other information about Au—including her name and date of birth—before the attack to steal her driver’s license number from Noblr’s website. Second, under New York law, a Social Security number is required to apply for unemployment benefits.² N.Y. Comp. Codes R. & Regs. tit. 12, § 473.1(f) (“Each claimant shall furnish his/her Social Security account number as a condition of eligibility for benefits.”). Finally, Au’s Social Security number did in fact become linked with the fraudulent application.

Taken together, these facts are strong evidence that the attackers already possessed personal information about Au before the Noblr cyberattack and gained additional personal information required to complete the application in cyberattacks unrelated to the incident involving Noblr’s quote system. Given that multiple attacks must have occurred, Au alleges no credible basis for why the attack on Noblr’s system was the source of the information used in the application for benefits. This case is therefore unlike *Zappos*, where the most the defendant could say was that some other data breach “*might* [also] have caused the plaintiffs’ private information

² The parties dispute the propriety of Noblr’s request that this court take judicial notice of the benefits application requirements as displayed on the New York State Department of Labor website. But given that the Social Security number requirement is confirmed by regulation, the court need not refer to the website to conclude that at least some personal information other than a driver’s license number is required to apply. Noblr’s request for judicial notice is therefore denied as moot.

to be exposed.” 888 F.3d at 1029 (alteration in original). Au has failed to prove that her injuries stem from “the challenged action of the defendant, and not ... the independent action of some third party not before the court.” *Lujan*, 504 U.S. at 560–61 (internal quotation marks omitted).

Finally, because Plaintiffs have not requested any further leave to amend, we decline to remand for further amendment of the complaint.

AFFIRMED.